State of California Department of Consumer Affairs

LEGAL AFFAIRS
400 R STREET, SUITE 3090
SACRAMENTO, CA 95814-6200

Legal Guide P-3

CREDIT IDENTITY THEFT: TIPS TO AVOID AND RESOLVE PROBLEMS

January, 1999

"Credit identity theft" or "identity theft" means the theft of a consumer's personal identification and credit information which the thief uses to gain access to the victim's credit and bank accounts and take over the victim's credit identity.

Credit identity theft is a growing consumer problem in California.

A recent *Consumer Reports* article describes a typical case of credit identity theft as reported by the victim:[1]

> An employee of a medical office where the victim received services obtained the victim's name and Social Security number from the victim's medical file. With this information, the thief allegedly was able to obtain lines of credit in the victim's name worth $10,000, rent an apartment, obtain utility service, and earn income in the victim's name. Prior to this, the victim's credit report was "spotless."
>
> The victim first learned that she was the victim of credit identity theft when she began receiving telephone calls from lenders and collection agencies demanding payment of numerous past-due credit accounts that she had not opened. As reported by the victim, her bank refused to refinance her home mortgage because she was a bad credit risk, and the Internal Revenue Service claimed that she owed taxes on income that the thief apparently had earned.
>
> It took the victim two years to have the negative credit information caused by the thief's activities removed from her credit report. The victim reported that during this time, the thief continued to use the victim's name, and creditors continued to press her for payment.

This Legal Guide explains how credit identity theft occurs; provides tips to avoid becoming a victim of credit identity theft; and suggests how to resolve problems if your credit identity is stolen.

I. DESCRIPTION OF CREDIT IDENTITY THEFT

A. Definition

Credit identity theft occurs when someone (the "perpetrator") wrongfully acquires and uses a consumer's personal identification, credit or account information. The perpetrator may use this information to obtain money, credit, goods, services and other things of value in the victim's name. The perpetrator also may use this information to gain access to the victim's bank accounts. The means by which the perpetrator obtains this information are discussed at B. below.

A consumer may not know that he or she has been a victim of credit identity theft for some time after the fact. The consumer often learns that he or she has been victimized after being refused an extension of credit. Typically, the victim's credit standing is seriously damaged by the perpetrator, and the victim's credit report becomes filled with negative credit information as a result. Consumers who are victims of credit identity theft have found it difficult to remove erroneous negative credit information from their credit reports and to re-establish their credit standing.

In the past, some law enforcement officials and credit reporting agencies did not consider the consumer to be the "victim" of credit identity theft because the consumer's liability for credit card losses generally is limited by federal law to $50 for each card (see explanation at III. below). They viewed the creditor or financial institution as the victim, although the consumer always has been the one who faces the emotional trauma and the often tedious task of re-establishing his or her

credit standing and removing erroneous information from his or her credit report.

A law that took effect on January 1, 1998, created the crime of "identity theft."[2] As knowledge of this new provision spreads, it should become clear to all that the *consumer* is the victim of credit identity theft.

B. How Credit Identity Theft Occurs

Credit identity theft can occur in daily consumer transactions in a variety of ways. For example:

Mail theft -- If a consumer leaves his or her credit card payment envelope in the mail box for the postal carrier to pick up, a thief may steal the envelope. The thief then may use the information from the credit card statement and the consumer's check to obtain credit in the consumer's name. A thief also may steal preapproved credit offers and convenience checks from a consumer's mail box and use the information contained in them to obtain credit in the consumer's name.

"Dumpster diving" -- If a business discards papers containing its customers' personal identification information (e.g., loan applications) without shredding them, a "dumpster diver" may retrieve this information from the business' dumpster (trash container). The thief then may sell the information or use it to obtain credit in the consumer's name. Similarly, if a consumer discards documents containing personal identification information (e.g., pre-approved credit offers) at home without destroying them, a thief may steal the information from the consumer's garbage can.

"Insider access" -- An employee of a business may wrongfully retrieve personal identification information that the business has collected for legitimate reasons. The employee then may sell the information, or use it to obtain credit information about customers, which the employee then uses to obtain credit in the consumer's name.

Purse or wallet loss or snatching -- A thief may steal, or the consumer may lose, the consumer's purse or wallet. The thief then may use the consumer's stolen personal identification information to obtain credit in the consumer's name.

Computerized information services -- A business that sorts, packages and sells personal identification information in electronic form may not safeguard the information adequately, or may sell it to purchasers that the business has not appropriately screened. The purchaser or thief then may use the information to obtain credit in the names of the consumers to whom the information relates.

Internet — Personal identification information that is available on the Internet can be accessed by a thief and misused to obtain credit in the victim's name.

A consumer's Social Security number (along with the consumer's name) is a key to tapping into the consumer's credit identity. Having obtained the consumer's personal identification information, the perpetrator then may apply for a new driver's license in the consumer's name, order new credit cards in the consumer's name to be sent to the perpetrator's address, obtain a copy of the consumer's credit report, and otherwise assume the consumer's credit identity.

Neglect by some retailers and creditors may contribute to a perpetrator's successful use of the victims' credit identity. For example, some retailers may not carefully check signatures on alternate identification given by consumers in check and credit card transactions, or may not check the validity of consumers' drivers' licenses when they apply for new credit.

II. HOW TO PROTECT AGAINST CREDIT IDENTITY THEFT

It is impossible for a consumer to prevent all distribution of his or her personal identification and credit information, or to exercise meaningful control over all of the possible uses of that information. Nonetheless, a consumer can take steps to reduce the risk of theft and misuse of his or her personal identification and credit information. For example:

Do not routinely carry your Social Security card, your birth certificate, your passport or more than one or two credit cards. When you must carry some or all of these, take special precautions to reduce the risk of loss or theft.

Always take credit card, debit card and ATM receipts with you. Never throw them in a public trash container. Tear

them up or shred them at home when you no longer need them.

Do not leave bill payment envelopes at your mailbox for the postal carrier to pick up. Install a lock on your mailbox if you live in an area where mail theft has occurred.

Tear up or shred unused preapproved credit card solicitations and convenience checks.

Carefully review your credit card statements and utility bills (including cellular telephone bills) for unauthorized use as soon as you receive them. If you suspect unauthorized use, contact the provider's customer service and fraud departments immediately.

Order your credit report each year from each of the three major credit reporting agencies (see the List of Resources below). Check each credit report carefully for accuracy and for indications of fraud, such as credit accounts that you did not open; applications for credit that you did not authorize; credit inquiries that you did not initiate; charges that you did not incur; and defaults and delinquencies that you did not cause. Check the identifying information in your credit report to be sure it is accurate (especially your name, address, and Social Security number).

Never give out your credit card, bank account or Social Security number over the telephone unless you placed the call and you have a trusted business relationship with the business or organization.

Guard against overuse of your Social Security number. Release it only when necessary -- for example, on tax forms and employment records, or for banking, stock and property transactions.

- Do not have your Social Security number printed on your checks. Do not allow a merchant to write your Social Security number on your check. (California law does not specifically allow or prohibit merchants from requesting and recording your Social Security number when you pay by check.)[3]
- If a business requests your Social Security number, ask to use an alternate number. Some businesses have systems to identify their customers that do not use Social Security numbers. If the business does not have such an alternate system, ask to use an alternate identifier that you will remember (for example, a combination of the letters of your last name and numbers). You can lawfully refuse to give a private business your Social Security number, but the business then can refuse to provide you service.
- If a government agency asks for your Social Security number, a Privacy Act notice should accompany the request.[4] This notice will explain whether your Social Security number is required or merely requested; the use that will be made of your Social Security number; and what will happen if you refuse to provide it.

If you do not receive your credit card statement on time (or if you do not receive a new or renewed credit card when you expect it), it is possible that an identity thief has filed a change of address request in your name with the creditor or the post office. Identity thieves do this to divert their victims' mail to the thief's address.

- Call the creditor to see if a change of address request has been filed in your name, or if additional or replacement credit cards have been requested on your account. If either has happened, inform the creditor that you did not make the request and instruct the creditor not to honor it.

- Call the post office to see if a change of address request has been filed in your name. If this has happened, immediately notify the Postal Inspector (see the "Postal Service" listing under "United States Government" in the white pages of the telephone directory).

If you shop on the Internet, use a secure browser which encrypts or scrambles purchase information, or place your order by telephone or mail.[5]

Check your Social Security Earnings and Benefits statement once each year to make sure that someone else is not using your Social Security number for employment. You can order this statement from the Social Security Administration (see the List of Resources below).

Consider having your name removed from marketing lists.

- The three major credit reporting agencies use information from credit reports to develop lists of consumers who meet criteria specified by potential creditors. You can request that your credit information not be used for these purposes.[6] Doing this will limit the number of preapproved credit offers that you receive.

- Credit card issuers often compile lists of marketing information about their cardholders based on their purchases. Under California law, you can request your credit card issuers not to disclose to marketers of goods any marketing information that identifies you.[7]

- The Direct Marketing Association (DMA) maintains lists of people who do not want to receive mail and telephone solicitations from national marketers. You can request that your name be added to the DMA's Mail Preference Service and Telephone Preference Service name-removal lists.

- See the List of Resources below.

Consider not listing your residence telephone number in the telephone book, or consider listing just your name and residence telephone number. If you decide to list your name and telephone number, consider not listing your professional qualification or affiliation (for example, "Dr.," "Atty.," or "Ph.D.").

Make a list of, or photocopy, all of your credit cards. For each card, include the account number, expiration date, credit limit and the telephone numbers of customer service and fraud departments. Keep this list in a safe place (*not* your wallet or purse) so that you can contact each creditor quickly if your cards are lost or stolen. Make a similar list for your bank accounts.

Cancel your unused credit cards so that their account numbers will not appear on your credit report. (If an identity thief obtains your credit report, the thief may use the account numbers to obtain credit in your name. To help avoid this problem, some credit reporting agencies "truncate" account numbers on credit reports.)

When creating passwords and PINs (personal identification numbers) do not use any part of your Social Security number, birth date, middle name, wife's name, child's name, pet's name, mother's maiden name, address, consecutive numbers, or anything that a thief could easily deduce or discover.

Memorize all your passwords and PINs; never write them in your wallet, purse or Rolodex.

Shield the keypad when punching in your PIN at an ATM or when placing a calling card call. This helps protect against "shoulder surfers" learning your code.

Install a lock on your mailbox at home, or use a post office box. This will reduce the risk of mail theft.

When you order new checks, pick them up at the bank instead of having them mailed to your home.

When you fill out a loan or credit application, be sure that the business either shreds these applications or stores them in locked files. These applications often contain all of the information that a dumpster diver or an unscrupulous employee needs to assume your credit identity.

III. WHAT TO DO IF YOU ARE A VICTIM OF CREDIT IDENTITY THEFT

A consumer must act quickly upon learning that he or she is the victim of credit identity theft. Acting quickly will help prevent the thief from making further use of the victim's credit identity, and may make the process of restoring the victim's credit standing less burdensome.

The victim should keep a log of the date, time and substance of all personal and telephone conversations regarding the theft. The log also should include the name, title and telephone number of each person to whom the victim speaks. The victim should follow up each telephone call with a letter that confirms the conversation and any agreed-upon action. The victim should send all correspondence by certified mail, return receipt requested, and keep a copy of each letter and each return receipt.

The following tips are offered to help a victim report and document the theft of his or her credit identity and to help the victim begin to rebuild his or her credit standing. Each case of credit identity theft involves unique facts and circumstances, and other than reporting the crime to the police, one victim will not necessarily take the same steps as other victims. If your credit identity has been stolen, you should review all of the following tips and choose those that are appropriate to your situation.

Report the crime to the police immediately. Effective January 1, 1998, California Penal Code section 530.5 classified identity theft as a crime.[8] Under legislation effective January 1, 1999, the crime of identity theft may be either a misdemeanor or a felony.[9] Ask the police to issue a police report pursuant to Penal Code section 530.5 on the theft of your personal identification information. Give the police as much information and documentation as possible. Creditors, banks, credit reporting agencies and insurance companies may require you to provide a police report to verify that you are a victim of the crime of identity theft.

- The full text of Penal Code section 530.5 is reprinted at the end of this Legal Guide. Not all law enforcement officials will be aware of this new law, or of the 1998 amendment under which identity theft may be a felony. If necessary, show this Legal Guide and the text of section 530.5 to law enforcement officials when you request a police report.

Call the fraud units of the three major credit reporting agencies (see the List of Resources below). Inform each credit reporting agency of the theft of your credit cards, account numbers or identifying information.

- Request that a fraud alert be placed in your file. Ask how long the fraud alert will remain posted in your file.

- Request that a victim's statement be added to your credit report -- for example: "My identification has been used to apply for credit fraudulently. Call me at _____ to verify any application for credit." Some credit reporting agencies require that you provide a copy of your telephone bill to verify your identity.

- Request a copy of your credit report from each credit reporting agency. The credit reporting agency must give you a free copy of your credit report if you have been denied credit.[10] If you certify to the credit reporting agency in writing that you believe that your file contains inaccurate information due to fraud, the credit reporting agency must give you a free copy of your credit report.[11] In other circumstances, each credit reporting agency can charge you $8.00 for your credit report.[12]

Check each credit report carefully when you receive it. Look for accounts that you have not applied for or opened; charges that you have not incurred; inquiries that you have not initiated; and defaults and delinquencies that you have not caused. Check your identifying information carefully — especially your name, address and Social Security number.

Request each credit reporting agency to remove all information that appears in your credit report as a result of the theft of your personal identification and credit information. It may take some time to have all of this erroneous information removed from each of your credit reports.

Ask each credit reporting agency to send you a copy of your corrected credit report. When you receive your corrected credit reports, verify that all of the erroneous information has been removed from each report, and that each report contains the fraud alert and victim's statement that you requested. It's a good idea to send a letter to each credit reporting agency every two-three months explaining that you are the victim of credit identity theft and asking that you be provided a free copy of your credit report. This will enable you to check your credit reports for new erroneous information, and for previously-deleted erroneous information that may have reappeared.

- After July 1, 1998, credit reporting agencies must block reporting of any information that a victim of identity theft alleges appears in his or her credit report as a result of the crime of identity theft. The victim must submit to the credit reporting agency a copy of a valid police report filed under Penal Code section 530.5 (described above).[13]

Call each of your credit card issuers to report that you are the victim of credit identity theft. Ask each credit card issuer to cancel your card and provide a replacement card with a new account number. Immediately follow up each telephone call with a letter that confirms the conversation and the action the credit card issuer has agreed to take.

- Ask each credit card issuer about the status of your account. Ask if the card issuer has received a change of address request, or a request for additional or replacement credit cards. If you have not filed a change of address request or requested additional credit cards, instruct the card issuer not to honor these requests.
- A consumer's liability for unauthorized use of a credit card cannot be more than $50.[14] The consumer must notify the credit card issuer promptly upon learning of the unauthorized use. Most creditors will waive (forgive) the $50 if the consumer notifies the creditor within two days after learning of the unauthorized use.
- Also call each credit card issuer or creditor that has opened a new account that you did not authorize or apply for. These accounts probably will be listed in your credit reports. Explain that you are the victim of credit identity theft, and ask each issuer and creditor to close the account immediately. Some credit card issuers and creditors may ask you to sign an affidavit or to submit a copy of the police report on the theft of your personal identification information. Ask each issuer and creditor to inform each credit reporting agency that the account was opened fraudulently and has been closed.

If your bank account information or checks have been stolen, or if a fraudulent bank account has been opened using your identification information, notify the bank and the check verification companies listed in the List of Resources below.

- Close your checking and savings accounts and obtain new account numbers.
- Ask the bank to use a new unique identifier for your accounts. Do not use your mother's maiden name, since this information is available in public records.
- Call the payees of any outstanding checks that you are not certain you wrote. The payee is the person or business to whom you wrote the check. Explain to each payee that you are the victim of identity theft and that you have closed your checking account for that reason. Ask each payee to waive (for-give) any late payment or returned check fee. Then send each payee a replacement check drawn on your new account and stop payment on the check that it replaces. It's a good idea to enclose a note with each check explaining why you are sending a replacement check and reminding the payee that the payee has agreed to waive the late payment or returned check fee (if the payee has agreed to do so).
- Get a new ATM card and PIN. Do not use your old password or PIN.
- A merchant may refuse to take your check on the advice of a check verification company (because the thief has written bad checks in your name). The merchant will refer you to one of the check verification companies listed below. Call the check verification company and explain the situation.
- If you cannot open a checking account because of the thief's activities, call ChexSystems (see the List of Resources below).

Notify your gas, electric, water and trash utilities that you are the victim of identity theft, and alert them to the possibility that the thief may try to establish accounts using your identification information. Provide similar notice to your local, long distance and cellular telephone services. Ask the utility and telephone services to use a new unique identifier for your accounts. Do not use your mother's maiden name, since this information is available in public records. If your long distance calling card or PIN have been stolen, cancel them and obtain a new account number and PIN.

If you have lost your driver's license, or if you suspect that someone may be using your driver's license number, contact your local Department of Motor Vehicles office (listed under "State Government" in the white pages of the telephone directory). It is possible to obtain a new driver's license number under limited circumstances (described in endnote 15 below).[15]

If your Social Security number has become associated with dishonored checks and bad credit, it is possible, in extreme cases, to obtain a new Social Security number.[16] In order to obtain a new Social Security number, your situation must fit the Social Security Administration's criteria for issuing a second Social Security number. See endnote 17 (below) for a general overview of these criteria.[17]

- If you suspect that someone else is using your Social Security number for employment purposes, request a copy of your Social Security Earnings and Benefits statement. If the statement confirms this use of your Social Security number, contact the Social Security Administration. (To order your statement, or to contact the Social Security Administration, see the List of Resources below.)

Be prepared for banks and credit grantors to ask you to fill out fraud affidavits to be notarized or signed under penalty of

perjury. You can ask to have the fees for notarizing documents waived or reduced.

If you suspect that an identity thief has stolen your mail or has filed a change of address request in your name, notify the Postal Inspector (see the "Postal Service" listing under "United States Government" in the white pages of the telephone directory).

If you have a passport, notify the passport office that the identity thief may apply for a new passport (see the "Postal Service" listing under "United States Government" in the white pages of the telephone book).

Other issues:

- Erroneous civil or criminal judgment: The actions of a credit identity thief sometimes result in civil or criminal judgments being entered against the victim. If you are a victim of credit identity theft, and have had an erroneous civil or criminal judgment entered against you, you should consult an attorney about vacating the judgment.

  A new law effective January 1, 1999 is designed to help victims of identity theft who have had erroneous criminal judgments entered against them. Under this new provision, if a credit identity thief has willfully obtained another person's personal identification information without that person's authorization, has used that information to commit a crime in addition to the crime of identity theft, and is convicted of that additional crime, the court records must reflect that the person whose identity was falsely used to commit the crime did not commit the crime.[18]

- Uncooperative creditor or credit reporting agency: Occasionally, a victim of credit identity theft may encounter a creditor or credit reporting agency that unreasonably refuses to cooperate with the victim as the victim seeks to restore his or her credit standing. For example:

  The victim may notify a creditor that he or she is the victim of credit identity theft, and may provide the creditor appropriate documentation, but the creditor continues to send report of debts incurred by the thief to the credit reporting agencies; or

  The victim may provide a credit reporting agency appropriate documentation and request the credit reporting agency to remove information from the victim's credit report that appears due to the theft of the victim's personal identification and credit information, but the credit reporting agency does not remove the erroneous information from the victim's credit report.

  If you are a victim of credit identity theft, and if you believe that a creditor or a credit reporting agency unreasonably or carelessly continues to report erroneous information that is the result of the theft of your personal identification and credit information, consider seeking assistance from an attorney.

- Demands to pay debts caused by the credit identity thief: Since the victim of credit identity theft did not incur the debts caused by the thief, the victim ordinarily should not pay any debt which is the result of the theft. If a debt collector demands that the victim pay such a debt, the victim should explain why he or she does not owe the debt, and should send the debt collector a follow-up letter. The victim should

consult an attorney if the victim receives demands to pay a debt caused by the identity thief, or if the victim receives notice of a legal action based on debts incurred by the thief.

- See the List of Resources below.

Other resources: "Coping With Identity Theft: What to do When an Imposter Strikes" (Privacy Rights Clearinghouse); "Identity Theft: What to do if it Happens to You" (California Public Interest Research Group and Privacy Rights Clearinghouse). (See the List of Resources below.)

IV. LIST OF RESOURCES

A. Victim Advice and Assistance

Privacy Rights Clearinghouse
1717 Kettner Boulevard
Suite 105
San Diego, CA 92101

Tel: (619) 298-3396
FAX: (619) 696-7477
Email: prc@privacyrights.org
Web: www.privacyrights.org

Fact sheets include "Coping with Identity Theft," "Identity Theft: What to do if it Happens to You" (co-authored by CalPIRG), "My Social Security Number: How Secure is It?" and "How Private is My Credit Report?"

California Public Interest Research Group (CalPIRG)
11965 Venice Boulevard
Suite 408
Los Angeles, CA 90066
Tel: (310) 397-3404

Email: watchdog@pirg.org
Web: www.pirg.org\calpirg

Publications: "Identity Theft: What to do if it Happens to You" (co-authored by the Privacy Rights Clearinghouse), "Theft of Identity: The Consumer X-Files."

Center for Law in the Public Interest
10951 W. Pico Boulevard
Third Floor
Los Angeles, CA 90064

Tel: (310) 470-3000
FAX: (310) 474-7083

Advice regarding credit identity theft; representation in selected cases.

Local Police Department
Look in the white pages of you telephone book under the "Government" listings.

Local County Bar Referral Service
Referral to local attorneys. Look in the white pages of your telephone book under "[_____ County] Bar Association" in the "Business" listings.

California Department of Consumer Affairs
Consumer Information Center

(800) 952-5210
(916) 445-1254 (Sacramento area calls)

General advice regarding credit identity theft;
referrals to other resources.

California Attorney General's Office
Public Inquiry Unit

(800) 952-5225

General advice regarding credit identity theft.

B. Credit Reporting Agencies

[The following addresses and telephone numbers are accurate as of December, 1998, but may change in the future.]

Experian (formerly TRW)

To report fraud: (888) EXPERIAN
[(888) 397-3742] (toll free number)
FAX: (800) 301-7196, or
Experian Consumer Fraud Assistance,
P.O. Box 1017, Allen, TX 75013
To request report: (888) EXPERIAN
[(888) 397-3742] (toll free number), or
P.O. Box 2104, Allen, TX 75013

To dispute information: Call number in credit report or (888) EXPERIAN [(888) 397-3742] (toll free number)

To opt out of preapproved offers and marketing lists: (888) 567-8688) (toll free number)

Equifax

To report fraud: (800) 525-6285

To request report: (800) 685-1111, or P.O. Box 740241, Atlanta, GA 30374

To dispute information:
Call number in credit report, or
P.O. Box 105873, Atlanta, GA 30384

To opt out of preapproved offers: (888) 567-8688 (toll free), or Equifax Options, P.O. Box 740123, Atlanta, GA 30374

Trans Union

To report fraud: (800) 680-7289

To request report: (800) 888-4213, or P.O. Box 390, Springfield, PA 19064

To dispute information: Call the number in the credit report, or use "investigative request form" that accompanies report order form

To opt out of preapproved offers: (888) 567-8688, or P.O. Box 97328, Jackson, MS 39238

C. Direct Marketing Association

To remove your name and address from national marketers' mail and telephone solicitation lists:

Direct Marketing Association
MAIL PREFERENCE SERVICE
P.O. Box 9008
Farmingdale, NY 11735

Direct Marketing Association
TELEPHONE PREFERENCE SERVICE
P.O. Box 9014
Farmingdale, NY 11735

D. Social Security Administration

To order your Social Security Earnings and Benefits statement:

(800) 772-1203, or
Social Security Administration
Data Operations Center
P.O. Box 7004
Wilkes Barre, PA 18767

To report that your Social Security number is being used by another person to obtain credit or for employment purposes:

Call or visit your local Social Security Administration office (call (800) 772-1213 for nearest location or see the "Social Security Administration" listing under "United States Government" in the white pages of the telephone directory). You can also call the Social Security Administration's Office of Inspector General, (800) 269-0271.

E. U.S. Secret Service

The Secret Service has jurisdiction over financial fraud cases, but usually does not investigate individual cases unless the dollar amount is high, or the victim is one of many people victimized by the same perpetrator or a fraud ring. See the "Secret Service" listing under "United States Government" in the white pages of the telephone directory.

F. Check Verification Companies

To report that your checks have been stolen or that bank accounts have been opened in your name without your consent:

CheckRite	(800) 766-2748
ChexSystems	(800) 428-9623, (800) 328- 5121 (regarding closed checking accounts only)
Cross Check	(707) 586-0551
Equifax	(800) 437-5120

National Processing Company	(800) 526-5380
SCAN	(800) 262-7771
Telecheck	(800) 366-2425, (800) 710-9898

*****

NOTICE: We attempt to make our legal guides accurate as of the date of publication, but they are only guidelines and not definitive statements of the law. Questions about the law's application to particular cases should be directed to a specialist.

Prepared by:
Legal Services Unit
January, 1999

ENDNOTES

1. "Are You a Target for Identity Theft?" Consumer Reports, September, 1997.

2. Penal Code section 530.5 (enacted by Statutes 1997, chapter 768 (AB 156 (Murray) and amended by Statutes 1998, chapter 488 (SB 1374 (Leslie)). The full text of this section is reproduced below.

3. Civil Code section 1725.

4. The Privacy Act of 1974, Sections 1 and 2, Pub.L. 93-579 (codified at 15 United States Code section 552a, note 1).

5. See, for example, Action Line Report, "Tips for Cybershopping," Direct Marketing Association, Inc., December, 1996.

6. 15 United States Code section 1681b(e).

7. Civil Code section 1748.12.

8. Penal Code section 530.5 creates the crime of "identity theft," defined as the willful, unauthorized obtaining of a consumer's personal identification information by another who uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services or medical information in the consumer's name without the consumer's consent. The full text of section 530.5 is reprinted at the end of this Legal Guide.

9. Statutes 1998, chapter 488 (SB 1374 (Leslie)).

10. Civil Code section 1785.17(b). In order to receive a free copy of your credit report, you must request it within 60 days after receiving the notice of denial.

11. 15 United States Code section 1681j(c) (limited to one free copy in any 12-month period).

12. Civil Code section 1785.17(a)(1).

13. Civil Code section 1785.16(k).

14. 12 Code of Federal Regulations section 226.12(b).

15. The Department of Motor Vehicles (DMV) will issue you a new driver's license number if a fraudulent or counterfeit license is obtained using your name and driver's license number, or if your lost or stolen driver's license is used by another to cash fraudulent checks or commit other crimes. You must be able to substantiate that your license or license number is being used in one of these ways. All of the requirements for obtaining a new driver's license number are explained in DMV's Fast Facts publication number FFDL-13, "The Requirements for Obtaining a New Number" (4-96). You can obtain this publication at your local DMV office.

16. "When Someone Uses Your Social Security Number," Published by Social Security Administration Regional Office IX, 75 Hawthorne Street, San Francisco, CA 94105 (February 1997).

17. To be assigned a new Social Security number, the number holder must provide evidence to the Social Security Administration showing that he or she is being disadvantaged by misuse of his or her Social Security number (for example, misuse of the Social Security number has caused the number holder to be subjected to negative economic or personal hardship). Generally, the evidence required is from one or more third parties documenting actual Social Security number misuses, as well as evidence documenting that the individual is being disadvantaged by the misuse.

For example, the number holder might be asked to submit a letter or other documentation from one or more creditors clearly stating that someone else is using the number holder's Social Security number to obtain credit, and a recent letter denying the number holder credit.

The evidence must show that the disadvantage is recent or ongoing (that is, the disadvantage has affected the individual within the past year or happened further in the past but continues). The evidence can show that the Social Security number misuse occurred in the past, but the disadvantage must be recent. Third party knowledge must include the basis for the third party's knowledge. The number holder also must provide evidence as is required for obtaining an original Social Security number. (Social Security Administration, Program Operations Manual System ("POMS"), RM 00205.001, 00205.25.)

18. Penal Code section 530.5(c) .

TEXT OF PENAL CODE SECTION 530.5

530.5(a) Every person who wilfully obtains personal identifying information, as defined in subdivision (b), of another person without the authorization of that person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services or medical information in the name of the other person without the consent of that person is guilty of a public offense, and upon conviction therefor, shall be punished either by imprisonment in a county jail not to exceed one year, a fine not to exceed one thousand dollars ($1,000), or both that imprisonment and fine, or by imprisonment in the state prison, a fine not to exceed ten thousand dollars ($10,000), or both that imprisonment and fine.

(b) "Personal identifying information," as used in this section, means the name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, or credit card number of an individual person.

(c) In any case in which a person willfully obtains personal identifying information of another person without the authorization of that person, and uses that information to commit a crime in addition to a violation of subdivision (a), and is convicted of that crime, the court records shall reflect that the person whose identity was falsely used to commit the crime did not commit the crime.

[Statutes 1997, chapter 768 (AB 156 (Murray)), as amended by Statutes 1998, chapter 488 (SB 1374 (Leslie)).]